Financial Management Service
Privacy Impact Assessment
Regional Operations (RO)
Name of Project: Secure Payment System (SPS)

Data in the System

1. Generally describe the information to be used in the system:

The information in SPS relates to payments made on behalf of Federal Program Agencies (FPAs) to individuals and business entities. For every payment, there is a payee name a payment amount, and a payment date. For most payments, there is a payee identifier (e.g., SSN, claim number, Taxpayer ID Number) and an address to which the payment is to be directed.

2. What are the sources of the information in the system?

FPAs provide all payment data.

a. What files and databases are used?

SPS will use the input certifications and payment files from the FPAs. These files *may* contain personal or Privacy Act information.

SPS will use a file of financial institution routing numbers for electronic payments. This file is provided by the Federal Reserve System. This file contains no personal or Privacy Act information.

SPS will use an internally created file of schedule numbers used, do eliminate the possibility of issuing erroneous duplicate payments. This file contains no personal or Privacy Act information.

SPS will use a file of Agency Location (or accounting) Codes. This file contains no personal or Privacy Act information.

b. What Federal Agencies are providing data for use in the system?

All FPAs for which FMS provides disbursing services (i.e., almost every Federal agency) submit data to SPS.

c. What State and Local Agencies are providing data for use in the system?

No State or Local Agency provides data to SPS.

d. What other third party sources will data be collected from?

No third party sources provide data to SPS.

e. What information will be collected from the taxpayer/employee?

SPS does not collect any information directly from taxpayers, employees, or other payees of Federal payments. All payment-related information is provided by the FPA requesting the payment to be made.

3. a. How will data collected from sources other than FPA records be verified for accuracy?

Payment data comes only from FPAs. Each FPA is responsible for the accuracy of the payment data submitted. FMS maintains no files as to entitlement for any recipient of a payment FMS issues at the request of a FPA.

b. How will data be checked for completeness?

Other than enforcing file format edits, FMS does not and cannot check the data for completeness.

c. Is the data correct? How do you know?

See 3.a and 3.b, above.

4. Are the data elements described in detail and documented? If so, what is the name of the document?

Yes. "SPS Requirements Document"

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

System Administrators, Database Administrators, System Operators, Developers, and Managers. Each end user will be programmatically restricted to view and process data only for his/her own agency (actually, at the Agency Location Code level). All transactions will be written to a permanent, unalterable audit log, which will include type of transaction, date/time, and user.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Each end user will be programmatically restricted to view and process data only for his/her own agency. Access is strictly on a need to know basis. All users at a given FPA can view all payment data for that FPA. Only Data Entry Operators can create, modify, or delete payment data. FMS users at Regional Financial Centers (RFC) can view payment data for all FPAs serviced by that RFC. All transactions will be written to a permanent, unalterable audit log, which will include type of transaction, date/time, and user.

Criteria and controls are contained in SPS requirements and architecture/design/development documentation. Procedures and responsibilities are contained in user manuals and SPS Rules of Behavior.

3. Will users have access to all data on the system or will the users' access be restricted? Explain.

Criteria and controls are contained in SPS requirements and architecture/design/development documentation. Procedures and responsibilities are contained in user manuals and SPS Rules of Behavior.

See #1 and 2 above. Users have access only on a need-to-know basis.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?

See #1 and 2 above. In addition, all legitimate users must access SPS using a PKI certificate. All SPS users must be added to SPS user tables by a System Administrator. Without both a PKI certificate and existence on SPS user tables, browsing is prohibited. As explained previously, FPAs are responsible for determining all entitlement to payments they certify. Therefore, SPS grants all users from a given FPA (ALC) access to data for that ALC.

5. a. Do other systems share data or have access to data in this system? If yes, explain.

SPS payment data is passed to subsequent FMS applications which 1) generate payments, and 2) provide a permanent record of the detailed payment inscription. Access to the FMS payment system is limited to authorized FMS RFC personnel. Access to the permanent issue record is restricted to authorized FMS and FPA personnel. FPA personnel are programmatically restricted to data at the ALC level.

b. Who will be responsible for protecting privacy rights of payees and employees affected by the interface?

The interfacing systems and data all reside on the FMS mainframe computer system. Mainframe security is provided by CA-Top Secret. CA-Top Secret is administered by trusted, cleared FMS security practitioners.

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

FPAs submit data to SPS. Each FPA has access to its own data. No International, State, Local, or Other agency shares data or has access to it.

b. How will the data be used by the agency?

FPAs submit payment request data. FMS issues payments for validated requests.

c. Who is responsible for assuring proper use of the data?

The FMS Chief Information Officer, who directs the FMS IT security program/policies/standards, in conjunction with the business owner (the Chief Disbursing Officer of the United States), is responsible assuring proper use of all SPS data.

d. How will the system assure that agencies only get the information they are entitled to?

See previous descriptions of role-based processing and compartmentalization of data at the FPA/ALC level. In addition, SPS will be required to pass stringent acceptance and quality assurance testing, in which requirements will be matched to a requirements traceability matrix. Also, SPS has contracted for independent security and integrity validation and verification testing.

Attributes of the Data

1. Is the use of the data both relevant and necessary ro the purpose for which the system is being designed? Yes

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? No

b. Will the new data be placed in the individual's record? Not applicable

c. Can the system make determinations about individuals or employees that would not be possible without the new data? Not applicable

d. How will the new data verified for relevance and accuracy? Not applicable

3. a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Not applicable

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain. Not applicable

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain

SPS payment data can be retrieved only at the aggregate schedule level. It cannot be retrieved within SPS by personal identifier. However, once a valid SPS users retrieve the aggregate data, (s)he can display the individual data.

5. What are the potential effects on the due process rights of payees of:

- consolidation and linkage of systems? Not applicable
- derivation of data? Not applicable
- accelerated information processing and decision making? Not applicable
- use of new technologies?

SPS payment data will be passed between FPAs and FMS over the internet. SPS is being designed with sufficient security controls in place to protect the privacy and integrity of the data.

How are the effects being mitigated?

SPS will employ a multi-layered approach of hardware and application software techniques and controls to protect the privacy and integrity of the data.

Maintenance of Administrative Controls

1. a. Explain how the system and its user will ensure equitable treatment of payees.

As FMS has no responsibility for payee entitlement of the payments it issues, FMS treats all payments equally. SPS cannot and does not validate payment identifiers, other than that they pass edit criteria for field lengths and formatting, because FMS does not have responsibility for or knowledge of individual payment identifiers and other payee information which could be regarded as sensitive or subject to the Privacy Act. All SPS payment request data is passed to one of several standard payment generation applications, depending on the type of payment involved (e.g., check, electronic).

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

SPS will be a client/server application. SPS will run on only one platform. All users run the same version of the application. FMS configuration management procedures will permit only one version, digitally signed, to be in production at any given time.

c. Explain any possibility of disparate treatment of individuals or groups.

Not applicable

2. a. What are the retention periods of data in this system?

Data is retained in SPS until 15 days after the payments are issued. Audit/archive logs are permanent.

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

All data is held electronically until it reaches maximum age (15 days). All records beyond the retention period are immediately and automatically purged. There are no manual procedures. "Procedures" are in requirements documents.

c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

The requesting FPA is responsible for the accuracy, relevance, timeliness, and completeness of the data. SPS enforces completeness through on-screen edits and validations of data fields. SPS maintains the data in encrypted form, with access limited to authorized users.

3. a. Is the system using technologies in ways that FPAs have not previously employed?

SPS will be browser based.

b. How does the use of this technology affect payee/employee privacy?

SPS is designed to be as secure as possible to preclude attacks and misuse of payment data.

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

SPS will not provide the capability to identify, locate, and monitor individuals.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

SPS will not provide the capability to identify, locate, and monitor groups of people.

c. What controls will be used to prevent unauthorized monitoring? Not applicable

5. a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

Treasury/FMS .002 – Payment Issue Records for Regular Recurring Benefit Payments

Treasury/FMS .016 - Payment Issue Records for Other Than Regular Recurring Benefit Payments

b. If the system is being modified, will the SOR require amendment or revision? Explain

Not applicable – new system